THE ETHICS OF FACIAL RECOGNITION TECHNOLOGY

Nurzhan Kanatzhanov

Overview

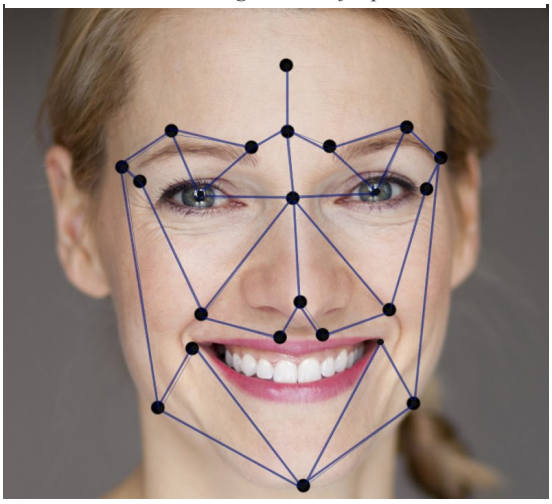
1. Introduction
2. How facial recognition technology works
3. Benefits of facial recognition technology in modern society
4. Ethical concerns behind the technology
5. Public opinion and legislation
6. The future of facial recognition technology/recommendations

Introduction

In 2015, the well-known mouthwash brand Listerine developed a smartphone application. While it sounds bizarre at first, Listerine launched the app as a part of a promotion to help blind people "feel" smiles using facial recognition technology. Their Smile Detector app analyzes the movement of one's face and determines if a person is smiling; the user's smartphone then vibrates and beeps, signaling that the person at the other end of the camera is smiling at them. Listerine released a short film to promote the app in which they let four blind people test it. One of them was a woman named Sarah who fought back tears of joy after she felt her one-year-old baby smile at her while playing.

Ultimately, a question came up from the app users: how exactly does facial recognition work?

Biometric "signature" of a person.



Simply put, facial recognition systems identify a person's face and analyze specific information based on various data, whether it is detecting mouth movement to create a smile, recognizing eye movement, or reading one's facial expression altogether. Think of the way *you* might recognize faces and other facial features. When describing someone, you would probably outline the shape of person's nose, eyes, eyebrows, cheekbones, jawline, how big or small their forehead, chin, and lips are. You would probably be good at identifying a friend, a family member, or a co-worker. But would you beat facial recognition technology? Probably not.

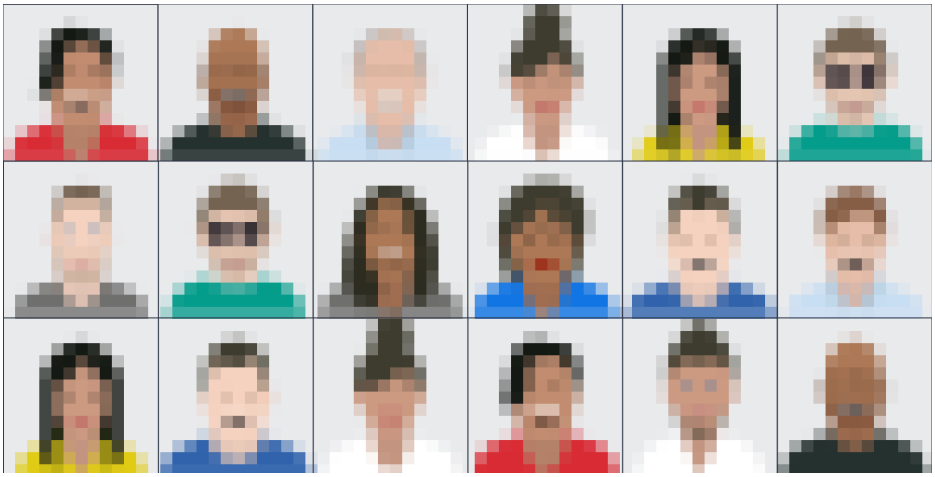
This article will explain to you how exactly facial recognition technology works, how it is used, and what benefits and controversies the technology entails with a final purpose of invoking an important ethical question: should we be concerned?

How It Works

Facial recognition technology works in a similar way to how you perceive human faces, but on a grand, algorithmic scale. Facial recognition technology uses biometrics

(unique body measurements and calculations) to map facial features from a digital image or video. The most common use of the technology is to verify personal identity by comparing facial data with huge databases of known faces to find a match (Symanovich). For instance, according to a 2016 Georgetown University Law Center study, “one in two American adults is in a law enforcement facial recognition network,” which accounts to roughly 117 million people (Garvie). There are five basic steps of facial recognition systems:

1. A picture of your face is captured from a digital image or video.
2. The technology reads the biometrics of your face: depending on software, key facial landmarks are identified (e.g. distance between eyes, distance from forehead to chin, etc.).
3. The facial landmarks are combined into a single result: your facial “signature.”
4. Your signature is then compared to existing databases of faces.
5. The software determines if your facial signature matches an existing image in a facial recognition database.



FBI has access to over 640 million photos of human faces through its vast database (Guliani).

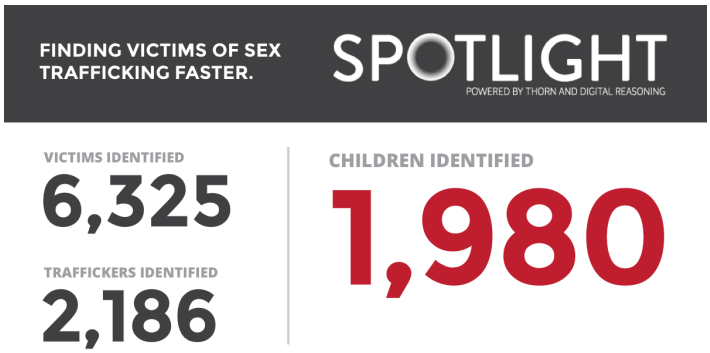
While facial recognition technology is constantly evolving as a useful tool, the uses of it vary drastically, both technologically and ethically. Below, a case-by-case outline of the benefits and concerns of the technology will be presented.

Benefits

Human Trafficking

Although the Listerine Smile Detector app was a great way to put facial recognition technology to use, its other uses to make this world smarter, safer, and more convenient will seem astonishing.

A non-profit Los Angeles startup called "Thorn" developed an app called Spotlight that helps find human trafficking victims. The app uses facial recognition technology to match people, and especially children under eighteen years old, found in sex-trafficking ads with police reports of missing persons. The technology behind the app is simple: the app scans the web for hundreds of thousands of escort ads, and then they upload the faces the children's faces that they find to a server hosted by Amazon, which then uses its own Rekognition technology—a cloud-based computer vision tool—to match the faces to missing children's posters. Spotlight is an amazing resource in the fight against human trafficking in the world where about 150,000 escort advertisements are posted online *every day*. While law enforcement simply does not have enough resources and capital to conduct searches on the massive human trafficking market, Spotlight is an invaluable, investigative tool to address that crime (Godlewski).



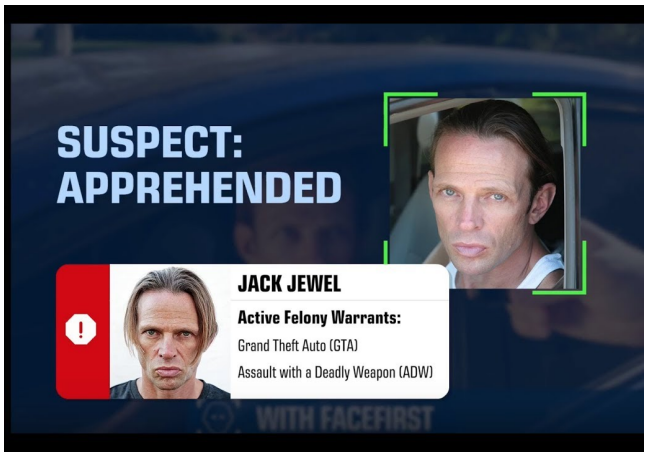
Spotlight helps identify over 8 children per day on average, reducing investigation times by 60%.

Spotlight is not the only app that helps law enforcement agencies improve security.

Law Enforcement

A company called FaceFirst utilizes facial recognition technology to allow police officers to instantly identify individuals from a distance. As mentioned before, with the large

number of photos in law enforcement databases, the mobile app that FaceFirst developed helps identify potential threats for public security. Say, during a regular traffic stop, a police officer could scan the driver's face from a safe distance, identify the driver, and see if he/she has any outstanding arrests, tickets, etc. Once they scan the driver's face with the app, they could call for backup without having to interact with the driver first.



FaceFirst claims to be highly accurate, scalable, secure, and private.

Drowsy Driving

Public safety seems to be one of the most important issues that facial recognition technology tries to solve. Engineers all over the world adjust to the ever-changing and progressing technology to deliver various solutions. In the case of transportation, policymakers are constantly looking for a solution to drowsy driving, something that is rarely caught or stopped. According to the American Automobile Association (AAA) research, about 9% of all monitored crashes were caused by drowsiness, whereas about 10.5% of crashes resulting in significant property damage, airbag deployment, and/or injury were connected to sleepiness (Gabriel); meanwhile, nearly half of American adults admit they have driven while drowsy, struggling to focus on the road (Searing). The belief that drowsy and distracted driving is a serious public health concern is true. Is there a solution? Facial recognition technology could make the roads safer. For instance, facial recognition technology is now installed in highway cameras and motorways to prevent drowsy and distractive driving in some areas of the world. These drowsy-driving prevention

More than 300,000 accidents a year are caused by drowsy driving.

apparatuses capture an incoming driver's face image after which the software would analyze the state of the driver. If the algorithm determines that the driver is either drowsy or distracted, a communication unit installed in the apparatus would contact appropriate services to alert of the driver's state that is dangerous for the driver and for others around them (Jeon). The closest police units would then pull over the drowsy driver, check in with them, and alert them of their potentially dangerous state, advising them to rest. This technology might save a lot of lives and prevent unnecessary crashes when drivers don't even notice that they have become drowsy or sleepy.

The cases noted above reveal the benefit that society would be able to enjoy with increased utilization of facial recognition technology. Next, I will present some examples of when public good is all but neglected for the benefit of some organization, government or private. These examples portray the use of facial recognition technology in ways that are not just in an ethical gray area, but many would argue are ethically wrong.

Concerns

Despite the benefits described above, facial recognition technology has been reported to be an extremely intrusive technology with multiple cases of its misuse. Are there any reasons to be concerned about your privacy with the prevalence of facial recognition technology? Definitely. One of the most fundamental arguments against the use of facial recognition technology by the government is the right to privacy, given by the Fourth Amendment to the US Constitution, to be free of "…unreasonable searches and seizures" (Amendment IV). With facial recognition technology, your facial data could be collected, stored, and distributed without your knowledge or permission. Your mood and eye movement could be analyzed by cameras with facial recognition technology. You could be tracked without even knowing that you are tracked. This all sounds like an Orwellian invasion of privacy (Bowyer).

Educational Use

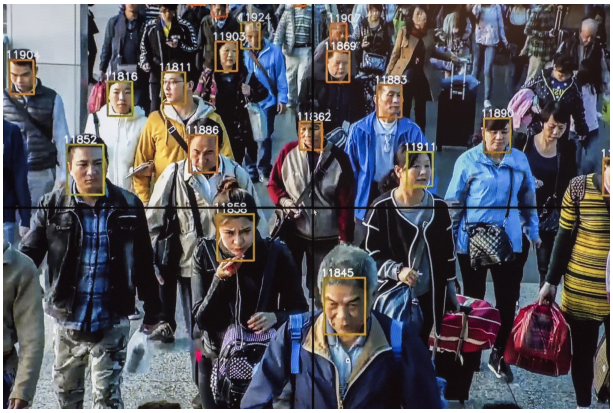
In the eastern China city of Hangzhou, about a year ago, a large local school installed cameras to monitor faces of students during lectures. The cameras assess the

students' attentiveness and facial expressions. Their main purpose was to determine whether they were enjoying lessons and whether they were paying attention. A news reporter asked one of the students what they think about the brand-new installation: "Since the school has introduced these cameras, it is like there is a pair of mystery eyes constantly watching me, and I don't dare let my mind wander" (Connor). The cameras record students' expressions to determine whether they are bored, focused or happy. Talk about "Big Brother" always watching you.

The system will send a notification to the teacher if it determines that a student is distracted.

Public Shaming

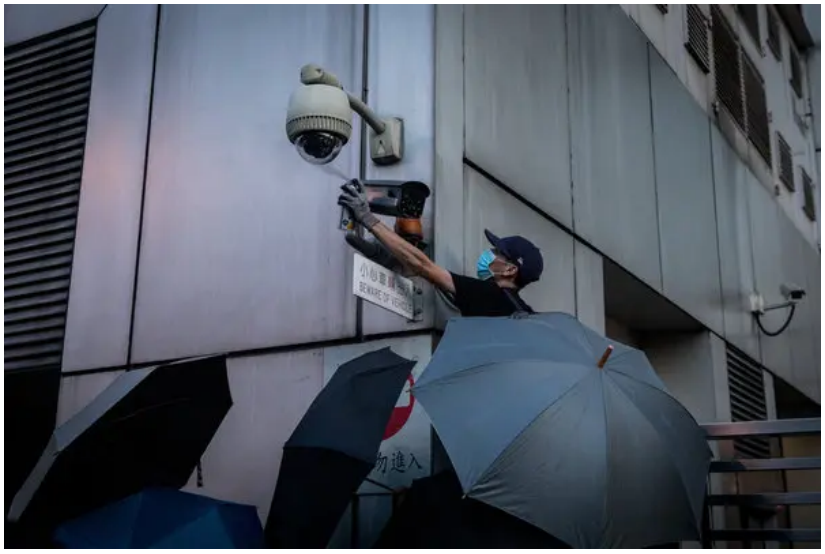
In another Chinese city of Shenzhen, we see this phenomenon: Shenzhen traffic police began displaying photos of jaywalkers on large LED screens at major intersections. With the help of artificial intelligence and facial recognition technology, jaywalkers will not only be publicly named and shamed, they will be notified of their wrongdoing via instant messaging—along with the fine. Facial recognition technology identifies the individual from a database and displays a photo of the jaywalking offense, the last name of the offender and part of their government identification number on large LED screens above the pavement. Public shaming, Shenzhen authorities say, incentivizes people to stop jaywalking, an issue that has been very persistent in large Chinese cities. Authorities then went as far as creating a separate website for jaywalkers, shaming them with the same information (Baynes).



The system displayed 13,939 jaywalking offenders at a single LED screen in Futian district in 10 months.

Protester Identification

Turning to the most recent events, facial recognition technology has been extremely controversial in a part of the world where people are fighting against the regime of surveillance. Protesters in Hong Kong constantly try to protect their anonymity in their fight for democracy and basic freedoms. Demonstration leaders are often seen wearing masks to thwart police cameras during protests that expanded over the past months against a bill allowing extraditions to China. Protesters spray-paint CCTV cameras on the streets and go as far as using military-grade lasers and smoke bombs to block off the vision of and confuse facial recognition cameras used by riot police. In a place where your face and identity are turned into weapons, it is truly a “cyber war against artificial intelligence” (Mozur).



A protester spray-painting a security camera in Hong Kong.

Not only does facial recognition technology and video surveillance serve as controversial talking points in technical issues such as privacy, security, and safety, but it also raises some eyebrows when you include the social issues behind it.

Misidentification

Amazon.com Inc., a US e-commerce tech giant, also did not miss out on the advancement of facial recognition software. Their cloud-based computer vision tool, Rekognition, is widely used by US government agencies like ICE, state police, and private entities for person identification. In a recent study, Amazon’s Rekognition had a hard time

identifying people with darker skin color, along with facial recognition systems made by IBM, Microsoft, and Google. For instance, the report suggests that "…the gender of 35% of dark-skinned women was misidentified, compared to 1% of light-skinned men such as Caucasians" (Wong). Jimmy Gomez, a California Democrat and one of the few Hispanic lawmakers serving in the US House of Representatives, was falsely matched with a mugshot of arrested criminals in a test done by the American Civil Liberties Union. He is currently one of the lawmakers pushing for ethical practices regarding facial recognition and addressing racial bias of the technology, so he decided to take part in ACLU's experiment, supporting his argument for the need of increased regulation. These practices bring a lot of concern. Facial recognition could disproportionately affect a large number of African Americans and other minorities due to the false identification of the technology. That is the scary part: facial recognition may be least accurate for those it is most likely to affect (Garvie).

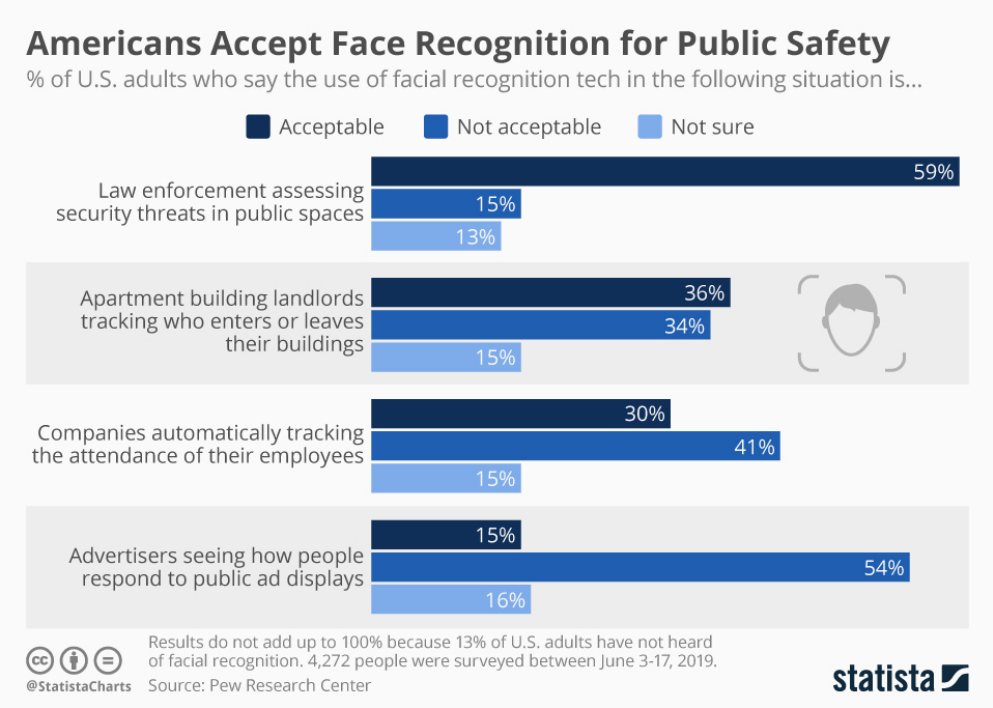
Jimmy Gomez claims mistaken identity could lead to a deadly interaction between law enforcement and that individual.

The controversy around facial recognition and its uses raises important issues in the area of its social impact. Its widespread application in everyday life and ever-changing nature raises serious security, privacy, and safety concerns for the general public.

Public Opinion and Legislation

Public Opinion

A study conducted by Pew Research Center in June 2019 shows the reactions of about 4,300 American adults towards the uses of facial recognition technology in various circumstances. The results are distinct:



While about 59% accept the use of the technology for public safety, only 15% find its commercial use acceptable.

Despite a high level of agreement of American adults towards public safety use of facial recognition technology—59% acceptance—the general public is still skeptical of its use in the hands of non-governmental companies, private entities, and individuals. For instance, agreement towards the technology dropped a whopping 23% after Americans who participated in the survey were asked if facial recognition would be used by landlords to track and control who enters and leaves their property. Even more surprising is that only 15% of American adults agreed that it is reasonable for advertising companies to track human attentiveness and response to public advertisement displays, whereas more than half responded that it was unacceptable. Ultimately, what drives this difference in public opinion?

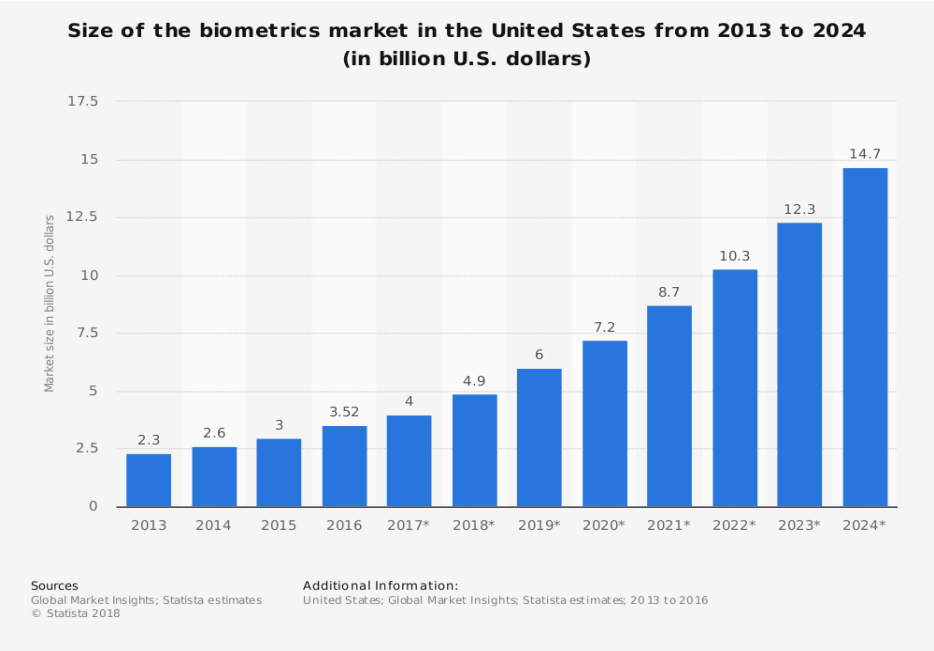
Public Distrust

The public distrust towards big tech could be attributed to the numerous scandals and controversies around data privacy and security leaks among some of the biggest companies in the world—Cambridge Analytica and Facebook, 100 million hacked bank accounts of Capital One, and 880 million leaked financial records of First America—all just in the past few years. On the other hand, the high level of acceptance for the use of facial

recognition technology by law enforcement agencies stems from the historically high level of trust that they have among the US public. In the post-9/11 context, facial recognition was and still is seen as a reliable technology and a high-tech solution to one of the most pressing problems facing the American nation—public safety. Alexandra Stikeman, an author for MIT Technology Review, wrote this in December 2001:

> Of all the dramatic images to emerge in the hours and days following the September 11 attacks, one of the most haunting was a frame from a surveillance-camera video capturing the face of suspected hijacker Mohamed Atta as he passed through an airport metal detector in Portland, ME. Even more chilling to many security experts is the fact that, had the right technology been in place, an image like that might have helped avert the attacks. According to experts, face recognition technology that's already commercially available could have instantly checked the image against photos of suspected terrorists on file with the FBI and other authorities. If a match had been made, the system could have sounded the alarm before the suspect boarded his flight.

The suggestion that facial recognition technology may have averted the September 11 attacks was a serious claim that government agencies and lawmakers had after the catastrophe. There was great appeal in the idea that any future attacks could be prevented by high-tech technology like facial recognition. Terrorist attacks served as a catalyst for the race to increase national security measures with billions spent on public safety and border control. Biometrics is a still a growing market today:



Biometrics market is projected to grow by more than three times from 2016 to 2024.

Out of the projected $14.7 billion, about the third of that is the market for facial recognition technology and biometrics related to facial features.

Legislation

With the growing biometrics market and the rapid advancement of facial recognition, the line between security and privacy has never been so thin. Today, there are virtually no concrete guidelines for the way facial recognition technology could be used in public spaces. With public concern towards its use, real-time facial recognition brings a lot of uncertainty in a society where data privacy and ownership has become a significant factor of one's safety, both online and in real life. Many legislators on the side of regulation of such intrusive technology call for better public reporting, transparency, and internal audits. In her book on the culture of surveillance in modern society, Kelly A. Gates, a professor of communications and science at UC San Diego, writes: "Making authoritative predictions about increasingly ubiquitous and intrusive surveillance techniques encourages public acquiescence, while suppressing alternative, less technocratic ways to address complex social problems and envision a better future" (Gates 6). There is a need for the public to understand how exactly facial recognition technology is developed, how and where it is installed and used, and whose interests are served in the process, as Gates proposes, instead of blindly believing in the power and sophistication of facial recognition technology.

So, how should authorities address the risks that facial recognition technology creates?

The Future of Facial Recognition Technology

When technology permeates almost all aspects of our daily lives, it is impossible to ignore its potential benefits and drawbacks. On the positive side, facial recognition technology makes the world safer, smarter, and more convenient by benefiting law enforcement and bringing immense advantage to end-users. On the negative side, however, it may be misused for personal benefit and impact people's privacy. As you can see, there is a fine line between the benefits and concerns of the technology. The general

public feels safe when facial recognition technology is used to access security threats in public spaces but is enraged if the technology is used to track their attendance in schools or jobs. Where is the balance?

Some opponents of the technology push for its regulation and uses in modern society. Today, local politicians on both sides of the aisle are drafting bills and passing laws that would limit the use of the controversial technology. Major cities like San Francisco and Oakland, CA, and Somerville and Cambridge, MA, have already passed laws that ban government use of the technology, primarily for analyzing pictures or videos for personal identification. While the movement for regulation is in its beginning phases, two top lawmakers—Rep. Elijah Cummings from Maryland (Democrat) and Rep. Jim Jordan from Ohio (Republican)—plan to draft a bipartisan bill on facial recognition, a rare case where both parties are working together (Ghaffary). Both Democrats and Republicans agree that the primary concern is the potential of facial recognition technology to infringe on civil liberties of American citizens, which can have negative effects on free speech. Advocates of the technology and law enforcement agencies, however, have argued that modern bans might be going too far, as dozens of police departments use facial recognition to prevent crime in more effective ways.

Ultimately, the future of the technology will depend on the decisions of policymakers to find the right balance between the usefulness of the technology and the basic right to personal privacy. While the demand for facial recognition grows, lawmakers must discover that balance, being mindful of the public discourse on the topic. If facial recognition technology is to be commonly used by all law enforcement agencies, citizens should press legislators for laws that would regulate it, protect civil liberties, and prevent its misuse and abuse.

Works Cited

Amendment IV. United States Constitution.

"Americans Accept Face Recognition for Public Safety." *Statista*, Statista Inc., 10 Sep 2019. Web.

Baynes, Chris. “Chinese Police to Use Facial Recognition Technology to Send Jaywalkers Instant Fines by Text.” *Independent*, 29 Mar. 2018. Web.

Connor, Neil. “Chinese School Uses Facial Recognition to Monitor Student Attention in Class.” *Telegraph UK*, 17 May 2018. Web.

Gabriel, Erin. “Drowsy Driving is a Factor in Almost 10% of Crashes, Study Finds.” *CNN*, 8 Feb. 2018. Web.

Garvie, Clare, et al. “The Perpetual Line-Up.” *Center on Privacy & Technology at Georgetown Law*, 2 Oct. 2016. Web.

Gates, Kelly A. “Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance.” *New York University Press*, New York, 2011.

Ghaffary, Shirin. “How Facial Recognition Became the Most Feared Technology in the US.” *Vox*, Vox, 9 Aug. 2019. Web.

Godlewski, Nina. “What Is Thorn Spotlight? Ashton Kutcher-Owned Software Aims to Help End Human Trafficking.” *International Business Times*, 15 Feb. 2017. Web.

Guliani, Neema Singh. “The FBI Has Access to Over 640 Million Photos of Us Through Its Facial Recognition Database.” *American Civil Liberties Union*, American Civil Liberties Union, 10 June 2019. Web.

Jeon, Byong-Hun. “Preventive Terminal Device and Internet System from Drowsy and Distracted Driving on Motorways Using Facial Recognition Technology.” US 20080291008 A1, United States Patent and Trademark Office, 27 Nov. 2008.

K. W. Bowyer. "Face Recognition Technology: Security Versus Privacy." *IEEE Technology and Society Magazine*, vol. 23, no. 1, pp. 9-19, Spring 2004.

“Listerine - Feel Every Smile.” *YouTube*, YouTube, 2 Nov. 2016.

Mozur, Paul. “In Hong Kong Protests, Faces Become Weapons.” *The New York Times*, 26 Jul. 2019. Web.

Searing, Linda. “The Big Number: 45 Percent of Americans Admit to Driving While Being Drowsy.” *Washington Post,* 28 Oct. 2019. Web.

Statista. “Size of The Biometrics Market in the United States From 2013 to 2014 (in Billion U.S. Dollars).” *Statista*, Statista Inc., 21 Feb. 2018.

Stikeman, Alexandra. “Recognizing the Enemy.” *MIT Technology Review*, 1 Dec. 2001. Web.

Symanovich, Steve. “How Does Facial Recognition Work?” *NortonLifeLock*, Accessed 20 Nov. 2019. Web.

Wong, Queenie. “Why Facial Recognition’s Racial Bias Problem Is So Hard to Crack.” *CNET*, 27 Mar. 2019. Web.